ABSTRACT OF THE DISCLOSURE

Secure protection and distribution of a personal identification number (PIN) is achieved by using a first encryption process only for PIN data and a second encryption process for non-PIN data. The first encryption process uses asymmetric encryption, where a public key is used for encryption of PIN data and a private key, held only by an authorizing agent, is used to decrypt the PIN data. The second encryption process uses a key which is available to an authentication requestor, such as merchants. A party seeking authentication of PIN data must forward the encrypted PIN data to an authorizing agent along with account data necessary to validate the PIN data. The authentication requestor is provided with a signal which is indicative of the verification status of the PIN data without being privy to the contents of the PIN data.